

## UNITED STATES DISTRICT COURT

for the  
Western District of WashingtonIn the Matter of the Search of  
*(Briefly describe the property to be searched  
or identify the person by name and address)*INFORMATION ASSOCIATED WITH CALL NUMBER  
(470) 312-0220 STORED AT PREMISES  
CONTROLLED BY AT&T CORPORATION

Case No. MJ18-432

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A.

located in the Southern District of Florida, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

*Code Section*  
18 USC 1029  
18 USC 1344

*Access Device Fraud*  
*Bank Fraud*

*Offense Description*

The application is based on these facts:

See Attached Affidavit.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


*Applicant's signature*

Peter Vogl, Senior Special Agent

*Printed name and title*

Sworn to before me pursuant to CrimRule 4.1.

Date: 9/17/18

*Judge's signature*City and state: Seattle, Washington

Brian A. Tsuchida, United States Magistrate Judge

*Printed name and title*

STATE OF WASHINGTON           )  
   )          SS  
COUNTY OF KING               )

## I. INTRODUCTION AND AGENT BACKGROUND

2. As part of my training with the USSS, I graduated from the Federal Law Enforcement Training Center ("FLETC") and the USSS Special Agent Training Program where I received specialized instruction on investigating financial crimes. My training included instruction on the investigation of financial crimes, including credit/debit card fraud, mail and wire fraud, access device fraud, and identity theft. Since August of 2015, my duties have included investigating counterfeit currency and access device crimes. I am also assigned to the Joint Terrorism Task Force.

3. I am familiar with, and have participated in, a variety of investigative techniques including, but not limited to, analysis of documentary and financial evidence, surveillance, the questioning of witnesses, the implementation of undercover operations, and execution of search and seizure warrants.

## II. PURPOSE OF THIS AFFIDAVIT

4. I make this affidavit in support of an application for a search warrant for information associated with a certain cellular telephone assigned call number (470) 312-0220 ("the SUBJECT PHONE"), that is stored at premises controlled by AT&T Corporation ("AT&T") a wireless telephone service provider headquartered at 11760 U.S. Highway 1, North Palm Beach, Florida. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) to require AT&T to disclose to the government copies of the information further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review the information to locate items described in Section II of Attachment B.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that AARON LAWS and others have committed violations of Title 18, United States Code, Section 1029 (Access Device Fraud) and Title 18, United States Code, Section 1344 (Bank Fraud).

6. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. I have not included every fact known concerning this investigation. I have set forth the facts that I believe are necessary for a fair determination of probable cause for the requested search warrant. This warrant application is to be presented electronically pursuant to Local Criminal Rule CrR 41(d)(3).

## IV. PROBABLE CAUSE

7. In October 2017, an investigator at J.P. Morgan Chase notified the Kirkland Police Department that their customers' credit card numbers had been fraudulently used to make unauthorized purchases with digital wallets.

8. Digital wallet services allow users to securely store their payment information and to complete financial transactions electronically without having to

1 physically swipe or insert a debit or credit card. Many digital wallet services work  
2 through applications on cell phones, such as Apple Pay or Samsung Pay. For example,  
3 after adding a credit or debit card to the Apple Pay application, a user can simply tap his  
4 or her cell phone to a compatible check-out register to make payments at retail locations.

5 9. According to J.P. Morgan Chase, many of these fraudulent digital wallet  
6 purchases were linked to the same digital wallet device IDs and phone numbers.

7 a. For example, on August 9, 2017, R.Z.'s credit card was fraudulently  
8 used to make a \$15,078.67 purchase at Staples in Seattle, Washington. This purchase  
9 was made using Samsung Pay, with a 24-digit digital wallet device ID,<sup>1</sup> on a device  
10 associated with the telephone number (503) 568-0458.

11 b. Similarly, on August 2, 2017, R.A.'s credit card was fraudulently  
12 used to make a \$34,850 purchase at Ben Bridge in Portland, Oregon. This purchase was  
13 also made using Samsung Pay, with the same 24-digit digital wallet device ID, also on a  
14 device associated with the telephone number (503) 568-0458.

15 10. Law enforcement obtained surveillance images from some of the retail  
16 locations where these fraudulent purchases were made and determined that the same  
17 individuals appeared to be involved in these crimes. I have reviewed these surveillance  
18 images and have identified AARON LAWS, by comparing these images to his Colorado  
19 driver's license photos, as one of the individuals involved in completing these fraudulent  
20 transactions.

21 **A. SPECIFIC EXAMPLES OF OFFENSES**

22 **1. VICTIM M.W.**

23 11. According to J.P. Morgan Chase, on April 14, 2017, a fraudulent  
24 transaction appeared on M.W.'s credit card. A charge for \$4,104.52 was fraudulently  
25 made at the Microsoft Store in Seattle, Washington. This purchase was made with Apple  
26

27  
28 <sup>1</sup> The digital wallet device ID was MTcwMzMxMDAwMjAwNTAyNzYw.  
Affidavit of Senior Special Agent Peter Vogl - 3

1 Pay, using a 48-digit digital wallet device ID,<sup>2</sup> on an iPhone associated with telephone  
2 number 206-402-7648.

3 12. According to information obtained from Microsoft, the \$4,104.52  
4 transaction involved the purchase of two Microsoft Surface Pros and a type cover.

5 13. The following surveillance image was obtained from Microsoft. I have  
6 identified the individual pictured in this surveillance image as LAWS:



18 **2. VICTIM G.I.**

19 14. According to J.P. Morgan Chase, on September 28, 2017, fraudulent  
20 transactions appeared on G.I.'s credit card. These transactions included a \$8,446  
21 purchase at the Apple Store in Portland, Oregon. These purchases were made with Apple  
22 Pay, on a device associated with the telephone number (206) 503-3690, using an iPhone  
23 8.

24 15. According to information obtained from Apple, the \$8,446 transaction  
25 involved the purchase of three MacBook Pros and one Apple watch. The following  
26  
27

28 <sup>2</sup> The digital wallet device ID was 04351C53F13D800163070298109398654CB9FE8EEDCFE1A6.

1 surveillance image was obtained from Apple. I have identified the individual pictured in  
2 this surveillance image as LAWS:



12 **3. VICTIM D.T.**

13 16. According to J.P. Morgan Chase, on September 16, 2017, fraudulent  
14 transactions appeared on D.T.'s credit card. These transactions included a \$5,459.23  
15 purchase at Best Buy in Tukwila, Washington. These purchases were made with Apple  
16 Pay, on a device associated with the telephone number (470) 233-9218, on a device  
17 identified as a "Jet Black iPhone."

18 17. According to information obtained from Best Buy, the \$5,459.23  
19 transaction involved the purchase of two MacBook Pros and several items linked to Xbox  
20 games. The following surveillance image was obtained from Best Buy. I have identified  
21 the individual pictured in this surveillance image as LAWS:

22  
23  
24  
25  
26  
27  
28



18. In completing this transaction, the purchaser entered their Best Buy Elite Plus Member ID as one belonging to Jason Jones.

**B. USE OF FALSE IDENTITIES**

19. In October 2017, a Kirkland Police Department Detective contacted the owner of 303 E. Pike St. #304, Seattle, Washington 98122—the address that had been listed on the Jason Jones Best Buy Rewards account linked to the fraudulent purchase on D.T.'s credit card.

20. The owner of that apartment stated that the unit was rented to Jason Jones of Florida and that Jones used the email address mkjonesj@gmail.com and the phone number 470-728-2475. After the Detective showed the owner surveillance images from some of the digital wallet thefts, the owner identified the subject in those images as his renter, Jason Jones. I have identified the individual depicted in these images as LAWS.

Affidavit of Senior Special Agent Peter Vogl - 6

UNITED STATES ATTORNEY  
700 STEWART STREET, SUITE 5220  
SEATTLE, WASHINGTON 98101  
(206) 553-7970



1           21. I obtained a copy of the driver's license issued by the Department of  
2 Licensing in Florida to Jason Michael Kenneth Jones in Port Charlotte, Florida. On this  
3 license, the individual pictured is a Caucasian male, who does not resemble LAWS.

4           22. Accordingly, I believe that Jason Jones is an alias used by LAWS when  
5 committing these offenses.

6           **C. LAWS' ARREST AND SEIZURE OF DEVICES**

7           23. On October 12, 2017, LAWS was arrested at the Southcenter Mall in  
8 Tukwila, Washington. An employee from Best Buy recognized LAWS from a  
9 surveillance image obtained from Ben Bridge in Tukwila, Washington that a Kirkland  
10 Police Department Detective had provided relating to another fraudulent transaction. The  
11 employee explained that a man resembling LAWS just left Best Buy and was entering the  
12 Apple Store.

13           24. Renton Police Department officers responded to the Apple Store and  
14 detained LAWS. After reviewing several surveillance images of LAWS, recognizing  
15 him as the individual they had detained, the Renton Police Department officers arrested  
16 LAWS and took him into custody. Upon searching LAWS incident to arrest, officers  
17 located a State of Washington identification card in the name of Justin Zipperer and a  
18 State of Colorado identification card in the name of AARON LAWS. Both cards  
19 appeared to have the same male, LAWS, depicted in the photos. LAWS also had two  
20 cellphones, which were seized upon arrest, and LAWS was booked into King County jail.

21           25. After LAWS was arrested, he posted bond, and never returned to King  
22 County for further court proceedings.

23           **D. AT&T RECORDS**

24           26. According to records obtained from AT&T, a "prepaid customer" was  
25 listed as the wireless subscriber for the SUBJECT PHONE since October 14, 2017. The  
26 email address listed for the subscriber is heavyweightfayt@icloud.com.

27           27. During the course of this investigation, I have learned that LAWS uses the  
28 username HeavyweightFayt.



a. For example, according to information obtained from Apple, pursuant to a warrant, an iCloud account associated with LAWS contained a photograph of three iTunes cards and a computer screen showing a communication stating “HeavyweightFayt: I have 2 100 dollar and one 50 dollar is that ok.”

b. Similarly, an iCloud account associated with LAWS contained a screenshot of heavyweightfayt's Instagram account, which includes a photograph of LAWS.

28. According to records obtained from AT&T, the SUBJECT PHONE sent and received multiple phone calls to the telephone number 404-710-4488. According to AT&T, this number is registered to H.A. During the course of this investigation, I have learned that H.A. is LAWS' significant other and mother of his child.

## V. TECHNICAL TERMS

29. In my training and experience, I have learned that AT&T is a company that provides cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including cell-site data, also known as “tower/face information” or “cell tower/sector records.” Cell-site data identifies the “cell towers” (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the “sector” (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate location of the cellular telephone but is typically less precise than other types of location information, such as E-911 Phase II data or Global Positioning Device (“GPS”) data.

30. Based on my training and experience, I know that AT&T can collect cell-site data about the SUBJECT PHONE. I also know that wireless providers such as

1 AT&T typically collect and retain cell-site data pertaining to cellular phones to which  
2 they provide service in their normal course of business in order to use this information for  
3 various business-related purposes.

4 31. Based on my training and experience, I know that AT&T also collects per-  
5 call measurement data, which AT&T also refers to as the “real-time tool” (“RTT”). RTT  
6 data estimates the approximate distance of the cellular device from a cellular tower based  
7 on the speed with which signals travel between the device and the tower. This  
8 information can be used to estimate an approximate location range that is more precise  
9 than typical cell-site data.

10 32. Based on my training and experience, I know that wireless providers such  
11 as AT&T typically collect and retain information about their subscribers in their normal  
12 course of business. This information can include basic personal information about the  
13 subscriber, such as name and address, and the method(s) of payment (such as credit card  
14 account number) provided by the subscriber to pay for wireless telephone service. I also  
15 know that wireless providers such as AT&T typically collect and retain information about  
16 their subscribers’ use of the wireless service, such as records about calls or other  
17 communications sent or received by a particular phone and other transactional records, in  
18 their normal course of business. In my training and experience, this information may  
19 constitute evidence of the crimes under investigation because the information can be used  
20 to identify the SUBJECT PHONE’s user or users and may assist in the identification of  
21 co-conspirators and/or victims.


**VII. CONCLUSION**

33. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41. I further request that the Court direct AT&T to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on AT&T, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

  
\_\_\_\_\_  
PETER VOGL  
SENIOR SPECIAL AGENT  
UNITED STATES SECRET SERVICE

The above-named agent provided a sworn statement attesting to the truth of the contents of the foregoing affidavit on 17 day of September, 2018.

  
\_\_\_\_\_  
HONORABLE BRIAN A. TSUCHIDA  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

**PROPERTY TO BE SEARCHED**

This warrant applies to records and information associated with the cellular telephone assigned call number (470) 312-0220 (“the Account”), that are stored at premises controlled by AT&T Corporation (“the Provider”), headquartered at 11760 U.S. Highway 1, North Palm Beach, Florida 33408.

**ATTACHMENT B****ITEMS TO BE SEIZED****I. Information to be Disclosed by the Provider**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A for the time period October 14, 2017 through the present:

- a. The following information about the customers or subscribers of the Account:
  - i. Names (including subscriber names, user names, and screen names);
  - ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
  - iii. Local and long distance telephone connection records;
  - iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;
  - v. Length of service (including start date) and types of service utilized;
  - vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");
  - vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and

1           viii. Means and source of payment for such service (including any credit  
2 card or bank account number) and billing records.

3           b. All records and other information (not including the contents of  
4 communications) relating to wire and electronic communications sent or received by the  
5 Account, including:

6           i. the date and time of the communication, the method of the  
7 communication, and the source and destination of the communication (such as the source  
8 and destination telephone numbers (call detail records), email addresses, and IP  
9 addresses); and

10           ii. information regarding the cell tower and antenna face (also known  
11 as “sectors”) through which the communications were sent and received as well as per-  
12 call measurement data (also known as the “real-time tool” or “RTT” data), if available.

13 **II. Information to be Seized by the Government**

14 All information described above in Section I that identifies AARON LAWS’  
15 residence, employment, or habitual location during the time period of October 14, 2017  
16 through the present that may facilitate his arrest for, proceeds derived from, and evidence  
17 related to violations of Title 18, United States Code, Section 1029 (Access Device  
18 Fraud), and Title 18, United States Code, Section 1344 (Bank Fraud).

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT  
TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)**

I, \_\_\_\_\_, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by AT&T Corporation ("AT&T"), and my title is \_\_\_\_\_. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of AT&T. The attached records consist of \_\_\_\_\_ (pages/CDs/megabytes)]. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of AT&T, and they were made by AT&T as a regular practice; and

b. such records were generated by AT&T's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of AT&T in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by AT&T, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature